

We claim:

1. A computing system for processing a transaction, the computing system comprising:

5 a server system, the server system being arranged to process information associated with the transaction; and

a client system, the client system being in communication with the server system, wherein the client system includes a key engine which is arranged to generate keys and the client system and the server system are arranged to cooperate to assess
10 risk associated with the transaction.

2. A computing system according to claim 1 wherein the server system includes:

a profiling engine, the profiling engine being arranged to receive information associated with the transaction, the profiling engine further being arranged to generate
15 features associated with keys associated with the transaction;

a clustering engine, the clustering engine being in communication with the profiling engine, the clustering engine being arranged to substantially cluster the features into secondary keys; and

a replication engine, the replication engine being arranged to compare the keys
20 to the secondary keys to identify differences between the keys and the secondary keys.

3. A computing system according to claim 2 wherein the replication engine is further arranged to encrypt the differences between the keys and the secondary keys.

25

4. A computing system according to claim 3 wherein the replication engine is further arranged to provide the encrypted differences to the key engine.

30

5. A computing system according to claim 2 wherein the server system further includes:

a first database, wherein the profiling engine is further arranged to store at least some of the information in the first database; and

a second database, wherein the replication engine is arranged to store the differences in the second database.

6. A computing system according to claim 1 wherein the client is arranged to

5 send the keys generated by the key engine as a transaction to the server system.

7. A computing system according to claim 1 further including a transaction engine, the transaction engine being arranged to facilitate communication between the server system and the client system.

10

8. A computer-implemented method for processing a current transaction, the computer-implemented method comprising:

receiving information associated with the current transaction;

generating features for a first set of keys associated with the current

15 transaction;

clustering the features into a first set of secondary keys;

comparing the first set of keys to a second set of keys, wherein the second set of keys are associated with at least one previous transaction;

comparing the first set of secondary keys and a second set of secondary keys,

20 wherein the second set of secondary keys is associated with the at least one previous transaction;

determining whether there are differences between the first set of keys and the second set of keys;

determining whether there are differences between the first set of secondary

25 keys and the second set of secondary keys;

encrypting the differences between the first set of keys and the second set of keys when it is determined that there are differences between the first set of keys and the second set of keys; and

encrypting the differences between the first set of secondary keys and the

30 second set of secondary keys when it is determined that there are differences between the first set of secondary keys and the second set of secondary keys.

9. A computer-implemented method as recited in claim 8 further including:
storing the differences between the first set of keys and the second set of keys
in a first database when it is determined that there are differences between the first set
of keys and the second set of keys; and

5 storing the differences between the first set of secondary keys and the second
set of secondary keys in the first database when it is determined that there are
differences between the first set of secondary keys and the second set of secondary
keys.

10 10. A computer-implemented method as recited in claim 8 further including:
sending the encrypted differences between the first set of keys and the second
set of keys to a key engine; and
sending the encrypted differences between the first set of secondary keys and
the second set of secondary keys to the key engine.

15 11. A computer-implemented method as recited in claim 8 further including
saving the information associated with the transaction to a second database.

12. A computer-implemented method as recited in claim 11 wherein the
information is saved to the second database by a profiling engine.

20 13. A computer-implemented method as recited in claim 8 wherein the features
for the first set of keys are generated by a profiling engine and the features are
clustered into the first set of secondary keys by a clustering engine.

25 14. A computer-implemented method as recited in claim 13 wherein the first set
of keys is compared to the second set of keys by a replication engine, and the first set
of secondary keys is compared to the second set of secondary keys by the replication
engine.

30 15. A computer-implemented method as recited in claim 14 wherein the
differences between the first set of keys and the second set of keys and the differences

between the first set of secondary keys and the second set of secondary keys are encrypted by the replication engine.

16. A computer-implemented method as recited in claim 15 wherein the profiling

5 engine, the clustering engine, and the replication engine are substantially separate.

17. A computer-implemented method for handling a local transaction, the computer-implemented method comprising:

receiving a local transaction from a source;

10 encrypting at least a portion of the local transaction into at least one local transaction key;

producing at least one enhanced key using the at least one local transaction key;

determining when the at least one enhanced key is a new key;

15 sending the at least one enhanced key to the source when it is determined that the at least one enhanced key is the new key; and

processing the local transaction with the at least one enhanced key using the source, wherein processing the local transaction with the at least one enhanced key include applying a measure of transaction risk.

20 18. A computer-implemented method as recited in claim 17 wherein producing the at least one enhanced key using the at least one local transaction key includes: applying the at least one local transaction key to a local key database.

25 19. A computer-implemented method as recited in claim 18 wherein applying the at least one local transaction key to the local key database includes:

initializing the at least one local transaction key to a first lock; and

operating on the lock with the at least one transaction key, wherein operating on the lock with the at least one transaction key at least partially creates the at least 30 one enhanced key.

20. A computer-implemented method as recited in claim 18 further including:

storing key information in a key database.

21. A computer-implemented method as recited in claim 20 wherein the key information includes encrypted key information.

5

22. A computer-implemented method as recited in claim 20 further including: modifying the local key database after processing the local transaction.

22. A computer-implemented method as recited in claim 17 further including:

10 sending the transaction to the source along with the at least one enhanced key.

23. A computer-implemented method for handling a current transaction within a client-server system, the client-server system including a client computing system and a server computing system, the computer-implemented method comprising:

15 receiving information associated with the current transaction on the client computing system;

producing enhanced keys from the information associated with the current transaction using the client computing system;

sending the enhanced keys from the client computing system to the server 20 computing system;

generating features for keys associated with the current transaction using the server computing system;

generating secondary keys associated with the features for keys associated with the current transaction using the server computing system;

25 determining whether the keys associated with the current transaction and the secondary keys associated with the features for keys associated with the current transaction differ from the keys and the secondary keys associated with a past transaction using the server computing system; and

30 modifying a key database based upon the determination of whether the keys associated with the current transaction and the secondary keys associated with the features for keys associated with the current transaction differ from the keys and the secondary keys associated with the past transaction.